UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Joseph W. Freeman et al.

Serial No.: Not Yet Assigned

Filed: (Herewith)

Title: REDUCING THE BOOT TIME OF A TCPA BASED COMPUTING SYSTEM WHEN THE CORE ROOT OF TRUST MEASUREMENT IS EMBEDDED IN THE BOOT BLOCK CODE

Group Art Unit:
Not Yet Assigned

IBM Corporation
Intellectual Property Law
3039 Cornwallis Road
Research Triangle Park, NC 27709

INFORMATION DISCLOSURE STATEMENT

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Information Disclosure Statement is being submitted in connection with the above-identified application for patent. Applicants submit herewith patents, publications or other information of which they are aware, which they believe may be material to the patentability of this application and in respect of which there may be a duty to disclose in accordance with 37 C.F.R. § 1.56.

While this Information Disclosure Statement may be "material" pursuant to 37 C.F.R. § 1.56, it is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists.

The attached form, PTO-1449, provides a listing of patents, publications, or other information as required by 37 C.F.R. § 1.98(a)(1).

A copy of each of the items identified on the attached Form PTO-1449 is supplied herewith, except for the U.S. Patents and the pending patent applications, for which no copies are being submitted.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.
Attorneys for Applicants

By:______________________________
Robert A. Voigt, Jr.
Reg. No. 47,159
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
1201 Main Street
Dallas, Texas 75250-0784
(512) 370-2832

In Place of FORM PTO-1449 (Modified)

LIST OF PATENTS AND PUBLICATIONS FOR APPLICANTS' INFORMATION DISCLOSURE STATEMENT

Serial No.: Not Yet Assigned
Applicants: Joseph W. Freeman et al.
Filing Date: (herewith)
Group: Not Yet Assigned
Atty. Docket No.: RPS920030150US1

Reference Designation

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
________AAA	US 20020152382 A1	10/17/02	Xiao	713	173	
________ABA	US 20020169976 A1	11/14/02	Schelling et al.	713	200	
________ACA	US 20020166061 A1	11/07/02	Falik et al.	713	200	
________ADA	US 20020169979 A1	11/14/02	Zimmer	713	200	
________AEA	US 20030037231 A1	02/20/03	Goodman et al.	713	2	
________AFA	US 20030037244 A1	02/20/03	Goodman et al.	713	189	
________AGA	US 20030037246 A1	02/20/03	Goodman et al.	713	191	
________AHA	6,138,236	10/24/00	Mirov et al.	713	200	
________AIA	6,266,809 B1	07/24/01	Craig et al.	717	11	
________AJA	6,304,970 B1	10/16/01	Bizzaro et al.	713	200	
________AKA	6,493,807 B1	12/10/02	Martwick	711	163	
________ALA						
________AMA						
________ANA						

FOREIGN PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes No
________AOA						
________APA						
________AQA						

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial

________ARA "Flash Lock Out," *IBM Technical Disclosure Bulletin*, Vol. 38, No. 01, January 1995, p. 343.

________ASA

________ATA

Examiner: Date Considered:

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Flash Lock Out

Disclosed is a means to prevent unauthorized code from changing the contents of Flash memory. At power-up, software in the Flash updates the Flash memory if needed, then locks Flash using a hardware-supplied register bit.

PowerPC* systems use Flash memory to store the boot code, some system vital product data, and power-on self test. Flash memory is writable; this is desirable so that field upgrades to Flash may be made without physically changing the part. However, Flash is exposed, and errant code could overwrite the memory and destroy the system's ability to boot up and run.

This exposure is eliminated on PowerPC systems as follows:

- The Flash comes up in an open (writable) state.
- During power-on, software in the Flash checks to see if a Flash update is required. A key sequence or special record on the boot media may indicate that an upgrade is called for.
- If an upgrade is needed, then the upgrade boot occurs and Flash is rewritten.
- The PowerPC system hardware supplies a register bit which powers on to a reset condition. When this register bit is written to 1, it cannot be reset except with a power-off-and-on.
- After a Flash upgrade, or after it is determined that no Flash upgrade cycle is needed, the software sets the lockout register bit, thus locking the Flash.

The system is now safe from any accidental rewrites of Flash memory. Write cycles to Flash while it is locked will be ignored.

* Trademark of IBM Corp.